alert Food and Beverage and Cybersecurity and Privacy Practices

Saul Ewing LLP

FEBRUARY 2017

Restaurant Chain Latest Victim of Data Security Breach

Authors:
April F. Doss
Caitlin P. Strauss

SUMMARY

In early February 2017, Arby's Restaurant Group, Inc. became the latest retailer to report that it has suffered a large data breach affecting approximately 1,000 corporate restaurants and impacting as many as 350,000 credit and debit card accounts. Initial reports indicate that the breach occurred through the use of malware that infected the restaurant chain's point-of-sales system, allowing attackers to remotely steal data from each credit card as it is swiped at the cash register. This latest attack on a restaurant chain offers a good reminder to those in the retail industry to take precautions to prevent similar breaches.

Comparable data breaches have occurred in recent years at retailers including Wendy's, Home Depot and others. The data breach involving Wendy's is the subject of a class action lawsuit in federal court in Pennsylvania brought against the restaurant chain by 26 financial institutions for allegedly failing to prevent a data breach. A judge recently held that the pending class action could not be dismissed at an early stage of the litigation.

With respect to Arby's, the company reports that it has brought in a computer securities firm and has removed the affected malware. Arby's has notified law enforcement and is urging its customers to check their credit card account statements for suspicious activity.

One of the most striking things about this breach is that, according to news reports, Arby's did not discover the breach on its own; the breach was brought to Arby's attention by an independent security researcher. Arby's did not learn that its systems were compromised until after an estimated 355,000 payment cards had been compromised. Unfortunately, it is all too common for companies to be unaware of significant cybersecurity incidents that compromise the confidentiality of data on their systems. The longer a vulnerability goes undetected, the greater the cost to the company, in terms of the amount of data compromised, dollar costs for investigation and remediation, and – most importantly – reputational harm and, often, loss of business.

Despite the widespread and growing nature of cybersecurity risks, there are a number of effective steps that companies can take to lower their risk. These include:

- Ensuring compliance with the standards that govern handling of payment card information;
- Managing the cybersecurity risk associated with your third party vendors;
- Maintaining effective personnel policies and training;
- Having an effective cybersecurity incident response plan; and
- Considering whether cybersecurity insurance might be an effective way to manage some of the risk.

When it comes to incident response, the following are a few key points to keep in mind: First, with breach notification laws in effect in 47 different states, compliance with all of the legal requirements can be complex. The state breach laws are triggered by the state of residence where the affected consumer lives, not by the state in which the company does business, so even a very small restaurant, grocer, or beverage company can find themselves in a situation where a relatively small data breach makes them subject to the breach notification laws of dozens of states. Second, time is of the essence. An immediate breach response can stop any further loss of data, and a quick investigation is necessary in order for companies to be able to meet the notification deadlines of the various data breach laws, some of which require very rapid notice.

How Saul Ewing Can Help Your Restaurant Stay Protected

Saul Ewing has a robust Cybersecurity and Privacy practice group that works closely with other firm practice areas, like our Food and Beverage lawyers. We provide a full range of legal advice on cybersecurity preparedness and incident response, and we can help you think strategically about the low-cost measures you can take to reduce your legal risk associated with cybersecurity threats and data breaches. Specifically, we provide advice on the legal and regulatory framework that applies to the specific types of information your company holds; review vendor contracts for cybersecurity risk; draft and review personnel policies and deliver personnel training; draft and review incident response plans, and lead or participate in tabletop exercises designed to test the effectiveness of those plans; and we assist with an insurance program assessment. Depending on the nature of our clients' needs, we can engage technical consultants on their behalf, who can help assess the overall health and status of current IT systems, and make recommendations regarding potential improvements.

For more information on these matters, please contact the authors or the attorney at the firm with whom you are regularly in contact.

This Alert was written by April F. Doss, Chair of the firm's Cybersecurity and Privacy Practice, and Caitlin P. Strauss, Co-Chair of the firm's Food and Beverage Practice. April can be reached at 410.332.8798 or adoss@saul.com. Caitlin can be reached at 215.972.7153 or cstrauss@saul.com. This publication has been prepared by the Food and Beverage and Cybersecurity and Privacy Practices for information purposes only.